Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 4082084, 18 pages
http://dx.doi.org/10.1155/2016/4082084

Review Article

Privacy Models in Wireless Sensor Networks: A Survey

J. M. de Fuentes, L. González-Manzano, and O. Mirzaei

Carlos III University of Madrid, Avenida de la Universidad 30, Leganés, 28911 Madrid, Spain

Correspondence should be addressed to J. M. de Fuentes; jfuentes@inf.uc3m.es

Received 23 February 2016; Accepted 8 September 2016

Academic Editor: Christos Riziotis

Wireless Sensor Networks (WSNs) are attracting attention from the research community. One of the key issues is to provide them with privacy protection. In recent years, a huge amount of contributions has been focused on this area. Surveys and literature reviews have also been produced to give a systematic view of the different approaches taken. However, no previous work has focused on privacy models, that is, the set of assumptions made to build the approach. In particular, this paper focuses on this matter by studying 41 papers of the last 5 years. We highlight the great differences appearing among related papers that could make them incompatible to be applied simultaneously. We propose a set of guidelines to build comprehensive privacy models so as to foster their comparability and suitability analysis for different scenarios.

1. Introduction

The widespread network availability in modern societies, as well as the proliferation of connected devices that are routinely carried out by people, highlights the ubiquitous facet of today information technologies [1].

As a result of the abovementioned trend, our world is being transformed into a smart environment. Almost everywhere, there is a small sensor, receiver, or transponder with communication and processing capabilities. In order for this *smartification* to take place, sensors become a key element. Thanks to sensors, it is possible to perceive environmental conditions (temperature, humidity, etc.).

In order for these sensors to be effectively deployed, the concept of Wireless Sensor Networks (WSNs) comes into play. WSNs have received a great attention from the research community. As of January 2016, a general survey from Akyildiz et al. collected more than 15,000 cites on Google Scholar [2]. Thus, it is clear that there is a huge community behind this topic.

In this regard, WSN privacy needs have already been surveyed by several authors. Chow et al. [3], Tayebi et al. [4], Rios et al. [5], Gupta and Chawla [6], Oualha and Olivereau [7], Conti et al. [8], Bista and Chang [9], Alemdar and Ersoy [10], or Al Ameen et al. [11] are representative examples of systematic literature reviews on the matter. All of them focus on the different techniques that are proposed by authors to address typical security and privacy needs.

The goal of this paper is rather different from previous ones. Instead of focusing on the approaches taken, this survey concentrates on the considered *models*. Models are formed of all assumptions made over the system. In a WSN scenario, three main sets of decisions can be identified (see Figure 1). First, general issues such as goals and threats have to be stated. Afterwards, how the network is supposed to operate has to be defined. Finally, the attacker capabilities and resources need to be specified.

It must be noted that different contributions may not work properly together if they rely upon different models. Thus, it is critical to have a clear view on the considered models to identify whether two or more mechanisms are compatible. To the best of the authors' knowledge, there is no such a survey in this field. The last contribution of this paper is a set of guidelines to build comprehensive privacy-related models. They will help to clearly define these models to improve the comparability (and compatibility, if it is the case) of different proposals.

To ensure the timeliness of our results, we have focused on 41 papers published in the last 5 years. Figure 2 shows the temporal distribution of the considered papers. It is clear that there are several papers (4 at a minimum) per considered year, which supports the soundness of our analysis.

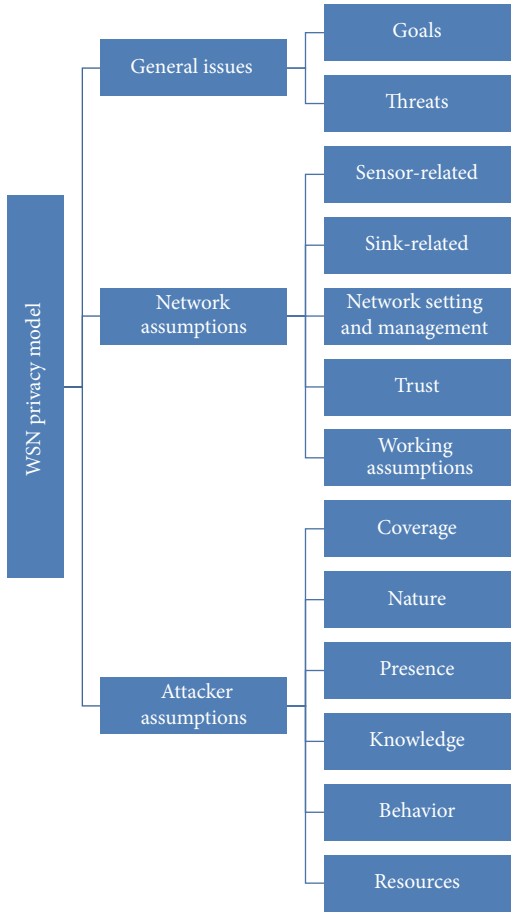

Figure 1: Privacy models in WSNs. Scheme of main decisions.

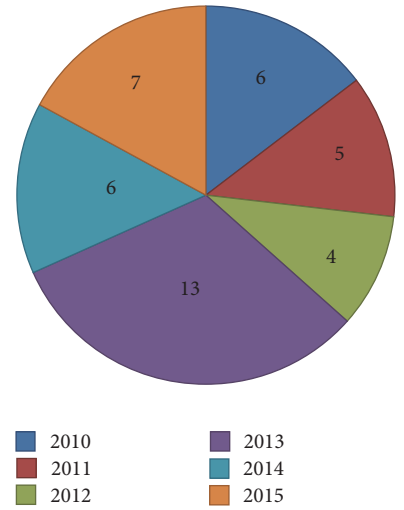

Figure 2: Distribution of papers per year.

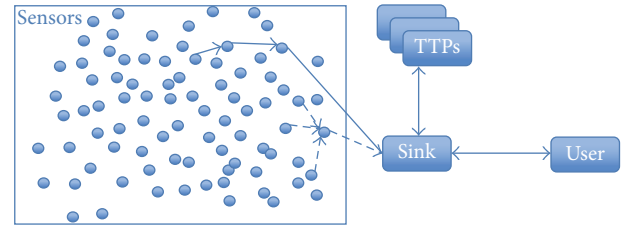

Figure 3: Scheme of a Wireless Sensor Network (WSN).

The paper is organized as follows. Section 2 gives a brief background on WSNs and the surveyed papers. Afterwards, the analysis is structured according to the decision sets shown in Figure 1. Thus, Section 3 focuses on the security goals and attacks that are at stake in the studied papers. Section 4 focuses on the assumptions made over the network itself. Section 5 describes the attacker capabilities. After the analysis on current works, Section 6 focuses on the guidelines to build privacy models. Finally, Section 7 concludes the paper.

2. Background

This section introduces the main concepts related to WSNs. Afterwards, the set of papers considered in this survey are briefly described. In particular, they are classified according to the followed approach. This enables showing the diversity of applied techniques, which supports the significance of the conducted survey.

2.1. Wireless Sensor Networks. A Wireless Sensor Network is formed by a set of sensors which are interconnected in an ad hoc fashion. Typically, it is assumed that sensors have a limited and nonremovable battery storage [2]. Their connectivity is usually ad hoc, so that they need to have a decentralized coordination. Thus, nodes share some information and carry out processing tasks in a distributed fashion. This is a typical feature of WSNs.

Apart from sensors, there are typically four entities in a WSN (Figure 3). On the one hand, the server or *sink* is the node that collects sensorial data. As it will be explored later on, this information may reach the sink either through direct routing (straight lines in Figure 3) or through some special sensors that collect data from surrounding ones (dotted lines in Figure 3). In order to make use of the network, the presence of a user is also assumed. Finally, Trusted Third Parties (TTPs) may also be considered to manage credentials and resolve disputes, among other issues.

These networks have been successfully applied in different applications and environments. Akyildiz et al. proposed a comprehensive enumeration of scenarios, ranging from military applications (e.g., reconnaissance) and environmental ones (e.g., tracking animals) to home uses (e.g., smart environments) [2]. In the last years, researchers have also explored their security issues related to their use in automated factories [12].

2.2. Classification of Considered Papers. The set of considered papers are devoted to different privacy-preserving goals. This section analyses the approaches followed on each work. This ensures that diverse techniques are considered and thus that

Table 1: Techniques. (x): technique assumed by authors as already existing.

	Encryption	Routing	Aggregation	Packet injection	Anonymity/k-anonymity/pseudonymity	Statistics
[44]		x		x	Anonymity	
[39]		x				
[30]	x	x				
[22]			x	x		
[28]					k-anonymity	
[25]	x					x
[52]		x		x		
[29]				x		
[31]		x	x		Anonymity	
[21]		x				
[34]					Pseudonymity	
[20]		x		x		
[49]	x		x			
[53]	x					
[16]	x (+ ring signature)				Pseudonymity	
[46]		x		x		
[50]					Pseudonymity	
[35]				x		
[54]			x			
[13]	(x)	(x)				
[14]	x			x	Pseudonymity	
[24]				x	Anonymity	
[38]		x				
[18]	(x)	x		x		
[47]		x				
[48]			x			
[26]			x			x
[42]	x				Pseudonymity	
[27]		x	x			
[45]	x		x			
[15]	(x)	x		x		
[19]	x	x		x	Pseudonymity	
[32]	x					
[23]	x	x		x		
[17]	x				Pseudonymity	
[43]	x		x			
[36]	x					
[33]	x					
[37]	x					
[40]	x	x	x			
[41]	x	x	x			

the survey is representative of the different directions in this field. Additionally, since papers are from the last 5 years, this section gives an up-to-date vision on the research trends in WSN privacy.

Figure 5 summarizes the different considered techniques, namely, encryption, routing, packet injection, aggregation, pseudonymity, anonymity/k-anonymity, and statistics. At a first glance, it may be seen that the total sum of techniques appearing in papers exceeds the size of the studied sample (i.e., 41 papers). This is because 25 out of 41 papers combine two or more techniques. Table 1 details this issue.

Around half of the papers make use of encryption. It is a reasonable decision since these mechanisms have already been applied to different network scenarios for long time ago. Therefore, existing algorithms may be adapted to the WSN constraints with relative easiness. One important remark is

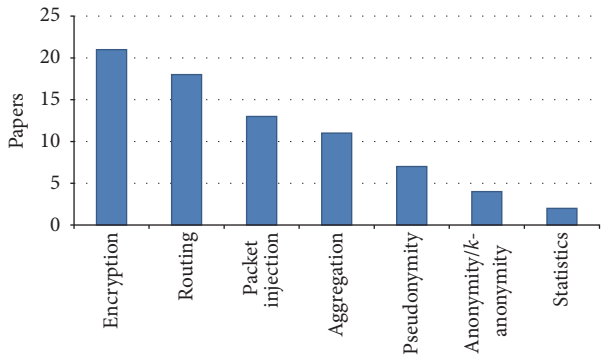

Figure 4: Classification of applied techniques.

that [13–15] do not explicitly adopt this mechanism as part of their approach. However, considering their description, it is clear that it comes into play.

Encryption is not the only pure-cryptographic mechanism at stake. Papers [16, 17] combine it with digital signatures. In particular, [16] applies ring signatures whereas [17] uses signcryption. This technique combines both digital signature and encryption at once. In both cases, the goal is to offer both sender anonymity and authenticity of data and its origin.

The second most popular technique is routing. More precisely, the preferred choice is to design a novel routing algorithm to demonstrate that the attacker cannot track a given packet back to its source. For this purpose, [15, 18–20] make use of fake sources and sinks to mislead the attacker. Another alternative is to use special kinds of routing such as tree routing. In particular, [20] proposes a diversionary tree routing in which packet paths cross themselves so that it is difficult for the attacker to track the actual path.

Proposed routing approaches may also leverage on the different types of considered nodes (see Section 4.1). As an example, in [21], routing is performed by specific nodes (called data mules) which are able to move around the network. This enables proposing algorithms which do not need to only rely upon static nodes.

Related to routing is the use of packet injection. In fact, most papers apply both techniques together. This approach bases on creating fake messages that are sent in the network. This technique comes at the cost of wasting some network and computation resources. Given that these are constrained aspects in WSNs, approaches are focused on how to apply this technique while maximizing the network lifetime. On the other hand, a critical aspect is to suitably inject messages to avoid real events tracking. Thus, papers such as [22] or [23] involve an opportunistic approach in which fake packets are only inserted when events come into play. Another option is taken by [24], in which packets are injected following a particular probability distribution. Systematic approaches in which randomness is not considered have also been proposed. For example, [18] makes a node to inject as many dummy packages as children nodes have.

Combining packet injection and encryption is not straightforward. One important remark in this regard appears in [25]. In that work, authors propose that encryption mechanism must be semantically secure, since it prevents the attacker from distinguishing between relevant messages and useless ones. This statement should be considered in all papers combining the two said techniques.

As the fourth most common technique, aggregation has gained research attention in the last years. One of the main reasons is that it allows reducing the amount of transmitted data. This procedure requires some form of organization among nodes. Thus, some of them become aggregators and have to carry out their operations. The process of selecting nodes as aggregators may either be done randomly or be the consequence of the applied routing algorithm. For example, aggregation trees are chosen in [26].

Another key reason for aggregating is that the sink might not always be present. This situation especially happens when the sink is moving around the network. Thus, in [27], a buffer-based aggregation is proposed while the sink is out of range.

The use of anonymity and pseudonymity is among the least applied techniques. It is worth mentioning that [28] focuses on a particular type of anonymity, called k-anonymity, in which each node becomes unidentifiable in a set of at least k elements. This lack of acceptance among researchers may be due to two reasons. On the one hand, it requires an additional identity management infrastructure to set pseudonyms for each node. This assumption may not be suitable for big-scale or harsh scenarios. On the other hand, full anonymity may not be required since nodes may get compromised. Thus, it may be potentially necessary to reveal the identity of the node in case it spreads false information or performs malicious actions.

The last technique is the use of statistical procedures for privacy preservation. This is only applied by [25, 26]. On the one hand, [25] proposes a statistical metrics to determine how private the location of the source is. For this purpose, it analyses the packets exchanged by the node. As the outcome is a metrics, [25] does not aim to solve the privacy problem by itself, but it is helpful to measure the effectiveness of other proposals. On the other hand, [26] enables determining whether a WSN is compromised or not by examining the result of an aggregation. To this end, the said result is statistically analysed, checking the likelihood of having been produced by a collusion of malicious nodes. Thus, [26] is a relevant complement for other aggregation mechanisms.

3. Privacy Goals and Threats

From a broader point of view, the most general aspects that have to be addressed by a privacy model are the pursued goals and the considered threats. This section focuses on each of these aspects for all the surveyed works. For the sake of clarity, goals are addressed in Section 3.1 whereas threats are studied in Section 3.2. Refer to Tables 2 and 3 for an in-depth comparison among papers.

3.1. Goals. Even if privacy seems a single requirement, it involves several goals that may be achieved to a different extent.

Table 2: Goals analysis.

	Location privacy: source/sink/both	Data confidentiality	Anonymity	Access control	Authentication
[44]	Both				
[39]	Source				
[30]		x (query)			
[22]		x (sensor data)			
[28]	Source				
[25]			x (source)		
[52]	Sink				
[29]		x (events)			
[31]		x (query)	x (aggregator)		
[21]	Source				
[34]			x		
[20]	Source				
[49]		x			
[53]		x			
[16]		x (events)			
[46]	Source				
[50]	Source				
[35]			x (source)		
[54]		x			
[13]				x	
[14]	Both				
[24]	Source				
[38]	Source				
[18]	Source				
[47]	Both				
[48]					
[26]		x			
[42]	Source				
[27]	Sink				
[45]					
[15]	Both				
[19]	Source				
[32]		x (query and query results)			x
[23]	Source				
[17]				x (query and query results)	
[43]					
[36]					x
[33]				x (query and query results)	
[37]					x
[40]		x			
[41]					

Table 3: Threat analysis.

	Eavesdropping/traffic analysis	Query revealing	Authentication and privacy: tracking (default)/impersonation (when noted)
[44]	x		x
[39]			x
[30]	x		x
[22]	x		
[28]			x
[25]			
[52]	x		x
[29]	x		
[31]	x		
[21]	x		x
[34]	x		x
[20]	x		
[49]	x		
[53]	x		
[16]	x		x
[46]	x		
[50]	x		
[35]	x		x
[54]	x		
[13]	x		x
[14]	x		x
[24]	x		x
[38]			x
[18]	x		x
[47]	x		
[48]	x		
[26]	x		
[42]	x		x
[27]			x
[45]	x		
[15]	x		x
[19]			
[32]		x	
[23]	x		x
[17]	x	x	x (impersonation)
[43]	x		
[36]			x (impersonation)
[33]	x		
[37]			x (impersonation)
[40]	x		
[41]			

Particularly, the considered papers address five privacy-related goals (Figure **??**): location privacy, data confidentiality, anonymity, access control, and authentication. We discuss each one separately.

The most common privacy goal in WSN-related contributions is source location privacy. The main reason behind it is that WSNs are usually devoted to detecting events. These events depend on the particular sensor capabilities: a fire may

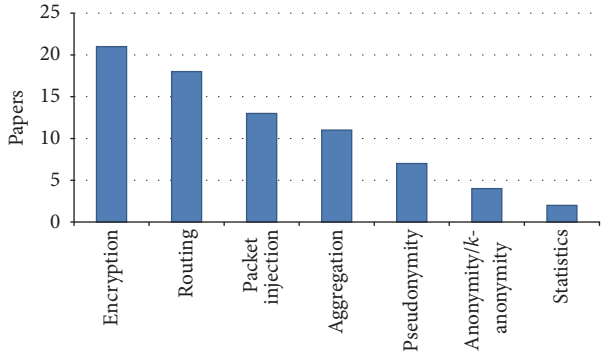

Figure 5: Classification of applied techniques.

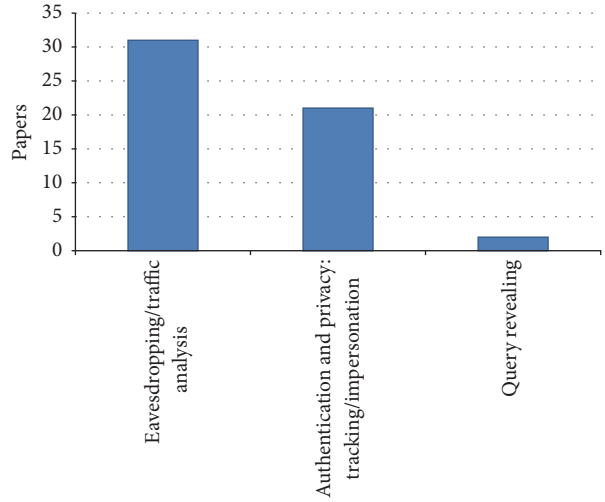

Figure 6: Considered threat distribution.

be the event if temperature sensors are in place, or a burglar appearance may be the target when presence sensors are used. One key remark is that the location of events may be relevant for unauthorized parties. For example, knowing where the alarm has been raised makes it easier for attackers to predict which zones may receive less attention for a period of time, since the staff will be focused on stopping the detected threat.

A similar reasoning can be applied to the sink node location. Given that most WSNs rely upon a unique node to collect their perceived events, discovering the location of such a node is critical to destroy the network. A typical example is the military scenario, in which sensors make alert on the presence of enemy troops. Once the sink is neutralized, all defenses will be unaware of the events perceived by perimetral detectors. Despite its potential practical relevance, it is the privacy goal with the lowest research attention. However, the interest rises when addressed jointly with source location privacy.

The second need in terms of relevance is data confidentiality. This is the focus of several papers, although they refer to different information pieces. There are three elements to protect. First, sensor data may be relevant itself [22]. Second, events, that is, special reporting by sensors when their perceptions are beyond a given threshold, are also critical [16, 29]. The third information element are queries and their results. The concept of query appears in WSNs in which there is a stakeholder (e.g., a supervisor) that can retrieve the network information on demand. Therefore, privacy preservation may be applied over the query itself, as it may leak hints on the interests of the stakeholder [30, 31]. On the other hand, given that query results show the network status according to that request, it is also a relevant matter for attackers [32].

Mainly related to queries, access control is a privacy-preserving goal in WSNs for a small subset of works. Particularly, only [13, 17, 33] are concerned with queries. The issue here is not only related to the confidentiality of information but also ensuring that only authorized parties may have access to that information.

Anonymity and authentication are among the least relevant goals. Papers [25, 34, 35] focus on providing sensor anonymity. This feature is related to the location privacy mentioned so far: if the node remains anonymous, it is not possible to distinguish it from others, thus avoiding location tracking. A similar approach is taken by [31], in which it is the aggregator node that remains anonymous. In this way, it is not possible to determine which node performed an aggregation. This is a similar protection to avoid compromising such a critical node within the network. However, this guarantee may be removed in case of misbehavior.

With respect to authentication, there are two possible variants, namely, entity authentication and data authentication. Papers [36, 37] offer mutual entity authentication, which means that both parties are sure on the identity of their counterpart. Data authentication is on the focus of [32]. It is noteworthy that this goal is specially relevant in aggregation-related approaches, since it is important to verify if the result of the operation is trustworthy.

3.2. Threats. Goals addressed in these papers have a direct link with the types of threats that WSNs may face. From a general point of view, the goals deal with data privacy and entities privacy. As a result, there are three main threats in this context (Figure 6): eavesdropping and query revealing (for data privacy) and authentication threats (for entities privacy).

Regarding data privacy, eavesdropping is by far the most common threat. It refers to the fact that an unauthorized entity may observe the contents of communication. One important aspect is that this threat might not be useful for learning the content itself but for discovering the involved nodes. This threat is usually referred to as *traffic analysis*, as it involves studying all traffic-related factors (e.g., sending-destination nodes, route taken, and frequency).

On the other hand, query revealing is at stake in a small subset of works. This trend is reasonable taking into account that only a reduced sample of considered papers dealt with the goal of access control to queries (recall Section 3.1).

Regarding entities' privacy, authentication threats are divided into tracking and impersonation issues. Tracking refers to the ability of the attacker to follow the physical situation of a given node. Recalling that location privacy is

the most relevant goal to achieve (cf. Section 3.1), the high impact of this threat is coherent. Most works are devoted to either rendering tracking impossible or at least reducing its success rate.

On the other hand, impersonation is addressed in [17, 36, 37]. This threat deals with the chance of a given entity to pretend to be another one. These works focus on avoiding this threat for access control purposes, thus ensuring that only authorized entities (and not third parties instead of them) can access some data.

4. Network Assumptions

Once goals and threats have been stated, the next issue to consider in a WSN privacy model is the network setting. Network assumptions may refer to the different elements that form the WSN or to external conditions in which the system is supposed to operate. This section focuses on these aspects. Sections 4.1 and 4.2 concentrate on sensors and sinks. How the network is managed is addressed in Section 4.3. Trusted elements are shown in Section 4.4 and finally Section 4.5 focuses on working assumptions. For the sake of clarity, tables contain an in-depth description of each aspect (Tables 4 and 5).

4.1. Sensor Assumptions. Sensor assumptions particularly focus on the type of sensor to apply, the information known by sensors, and sensors behavior.

The main aspect is that most works do not make any consideration regarding the type of sensors. In particular, only 4 papers mention that sensors must be static. On the other hand, paper [29] specifies that sensors are moving but at a uniform constant speed. The rest of the papers simply make no distinction. It must be noted that this decision has a direct impact in the soundness of the approach taken. One example is proposing a routing-based solution, that is, a specific mechanism to route packets in such a way that they avoid typical threats such as eavesdropping. If nodes are moving, there is a nonstraightforward need to maintain the routes. Without an explicit decision on this matter, this aspect may be overlooked.

Regarding the information known by sensors, a total amount of 16 papers makes a statement in this regard. There are three main elements that are explicit, namely, location, cryptographic keys, and identifiers. With respect to location, 4 papers assume that sensors know their own location (e.g., [38]) whereas 2 also consider that of the sink. Additionally, two papers determine that sensors know the identifier of the area in which they are placed; this is a relaxed form of location knowledge. Concerning keys, 9 papers assume that nodes know (from the beginning) either a shared key with the sink (e.g., [39]) or at least the sink's public key (e.g., [30]). In both cases, this is necessary to allow a confidential communication between these parties. Finally, 3 papers mention that each sensor has a unique identifier. This has direct implications in terms of the degree of privacy that has to be achieved; if sensors need to use such an identifier, it is necessary to build a mechanism to avoid revealing it to unauthorized parties.

With respect to the sensors behavior, there are two issues to note. First, several papers consider different classes (or roles) among sensors. These classes are linked to the type of mechanism, that is, considered. One typical assumption is that there are specific roles with extended attributions. As an example, aggregation nodes are in charge of receiving and putting together all information received from regular sensors [40, 41]. The second note regarding their behavior is that three papers assume that sensors are synchronized with the sink. Given that these networks may involve hundreds or thousands of nodes, such an assumption heavily limits the applicability of the proposal to specific scenarios.

4.2. Sink Assumptions. Sinks have particular properties to study. Specifically, the amount of entities that play the sink role, as well as the sink behavior, are analysed in the following.

The existence of a sink is mentioned in the vast majority of considered papers. However, they have great differences concerning its nature. One of the first aspects is that the amount of sinks is not usually explicit. Although several authors highlight that this is a single entity (e.g., [42, 43]), [30, 32] assume that there are several instances of it. Moreover, this issue is also part of the approach taken by authors in [18], as they propose several fake sinks to protect the single actual one.

The sink behavior is also subject to assumptions. Particularly, papers such as [15] consider that it is a static entity, whereas other authors [27] consider a moving one. In between, [44] admits both variants.

4.3. Network Setting and Management. WSNs are usually characterized by their simplistic network scheme in which the information flows between two entities, namely, sensors and sink(s) (recall Section 2). However, this vision hides different network topologies that are assumed by authors.

One outstanding organization scheme is the use of clusters or cells. In this way, sensors are separated into groups, usually based on their actual location. The typical setting is that there is one cluster head which is in charge of intercluster communication, whereas intracluster communication is direct among members. This setting is adopted by 9 of the considered papers, such as [45].

Apart from clusters, ring schemes are also considered in [31, 46]. Thanks to rings, nodes are virtually connected to another pair of neighbours (precedent and posterior in the ring). It is clear that this organization has a great impact on routing. However, to decrease predictability, some authors consider that sensors are organized into several rings and messages may flow from one to another.

It is noteworthy that an explicit mention to the network topology is not always given. Moreover, two papers state that their approach is applicable to any network topology [28, 47].

The last critical mention in this regard is the routing assumptions. Even if routing is one of the key mechanisms proposed by authors in recent years (see Section 2.2), there are several routing-related assumptions in the considered papers. Particularly, [44] assumes that communication from sensors to sink is done by flooding. In order to route packets, they rely

Table 4: Network assumptions: source and sink issues.

	Sensors: static/moving	Sensors: known info	Sensors: behavior	Sensors: capabilities	Server/sink
[44]					One, static, or moving
[39]		Shared key with sink	Cluster head and cluster members		
[30]		PK server			Set of independent, mutually untrusted servers
[22]		Global secret			
[28]		Own location Server location	Cooperate among themselves		Untrusted server
[25]			They broadcast fake messages		
[52]					
[29]	Moving sensors (uniform constant speed)				
[31]		Shared key with an "operator" which works through a gateway (or directly if it is close enough)	Leaf nodes and aggregator nodes		
[21]	Static ones and moving ones (data mules)	Own location (data mules)	Data mules do not communicate with each other. They move randomly	Greater communication coverage (data mules)	
[34]					
[20]		Own location, neighbours location, sink location			
[49]			Leaf nodes and aggregator nodes		One
[53]	Moving				
[16]					
[46]					One
[50]	Static	Unique ID	Cluster heads randomly chosen		
[35]		Predistributed shared key with any other node and with the base station			
[54]	Static (same cluster)		Cluster head and cluster members		Unconstrained
[13]					Privacy-enhanced base station
[14]			They can masquerade their MAC They are synchronized		One
[24]		Cell ID	Cluster head and cluster members		
[38]		Area ID			
[18]					One real, several fake
[47]	Static ones and moving ones			From low resources to high resources	
[48]					
[26]					
[42]		ID and location			One
[27]		Shared key with sink			Moving

Table 4: Continued.

	Sensors: static/moving	Sensors: known info	Sensors: behavior	Sensors: capabilities	Server/sink
[45]			Cluster heads and cluster members		
[15]	Static			Limited	Static
[19]	Static	Unique ID, shared key with sink, key for IBC		Limited	Static
[32]		Unique ID, shared key with user	Synchronized with sink		Several, untrusted
[23]					One but several allowed
[17]		Public key of owner and TTP			
[43]		Shared key with neighbours			One
[36]		Long-term key shared with the sink		Vulnerable to tampering	High resource, tamper-resistant
[33]			Synchronized with sink		One
[37]					Unconstrained Secure channel with authentication server
[40]			Leaf nodes and aggregator nodes		
[41]			Leaf nodes and aggregator nodes		

on an initial beacon sent by the sink at the beginning. In order to prevent overloading the network and, more specifically, the capacity of nodes, each one applies a policy to decide on whether to accept or reject the packet.

4.4. Trust Issues. Trust issues are also controversial. These are specially relevant since they identify which elements are reliable. Sensors and sinks are two of the elements that may or may not be trusted. In particular, [28, 48] assume that sensors and their connectivity are trusted, whereas [23, 36] do the same for the sink. On the contrary, papers such as [30, 32] consider that they are untrusted.

On the other hand, the network itself (i.e., communication channels) may be trusted as well. In particular, [44] assumes that the network is trusted for a period of time $T_{\min}$ after deployment of nodes. The last aspect to consider in this regard is the use of third parties and, in particular, the existence of Trusted Third Parties (TTPs). Several papers assume that there are authentication managers or other related entities. However, it is remarkable that [33] does not assume the existence of TTPs. This is interesting to ensure the applicability of the proposal in harsh environments (e.g., military scenarios).

4.5. Working Assumptions. Working assumptions are statements made about the status of the system, particular features of the scenario, or elements that are supposed to exist for the mechanism to operate properly. There are essentially two aspects: cryptographic and contextual aspects. Regarding cryptography, key management is sometimes taken for granted [20, 37]. A similar assumption is made in [49], which considers that a random key distribution scheme has already been applied.

Contextual aspects are related to how the scenario has to be. In this regard, the main issue is to define how events will happen. Two main decisions are taken in this regard. First, [31, 50] consider that time is slotted and that only one event may happen per slot. On the other hand, [29] assumes that events follow a probability distribution, initiate in the WSN perimeter, and end at some point inside the network. Thanks to these decisions, simultaneous or truly random events are not considered. Even if they impact the suitability of approaches for some realistic settings, other scenarios are totally applicable. For example, WSN-enhanced monitoring facilities in which measurements are taken periodically (say 5 seconds) may be compatible with the slotted-time assumption.

5. Attacker-Related Assumptions

Previous sections have focused on the privacy goals and threats and how the network is organized. This section addresses the last group of assumptions (recall Figure 1): attacker capabilities. They are critical to assess the degree of impact that threats may have. To make this analysis, the criteria by Back et al. (coverage, nature, and presence) are taken as a basis [51]. Furthermore, its assumed knowledge and behavior are also studied. Table 6 shows the analysis per paper.

The attacker coverage refers to its area of influence. Typical assumptions in this regard are that the attacker is *local* or *global* (Figure 7). The most common assumption is to have global attackers that can affect the whole network

Table 5: Network issues: management and trust.

	Network	Clusters/regions	Trusted issues	Working assumptions
[44]	Sensor-sink communication by flooding Routing bases on an initial beacon Each neighbour decides to accept/reject a packet using policy		Network is trusted for a period T_{min} after deployment	Set of authentication-encryption protocols in use
[39]		x		
[30]		x		
[22]	Tree routing			
[28]	No need for any specific topology Communication with server is anonymous		Sensors and sensor-sensor connectivity	
[25]				
[52]	The destination ID for each packet (i.e., the sink) is encrypted			
[29]				Events follow a probability distribution; initiate on a random location of the WSN perimeter; eventually terminate within the network
[31]	Ring	x		Time is slotted, one event per slot
[21]		x		
[34]				
[20]				Key management exists
[49]				Random key distribution scheme (e.g., Gligor)
[53]				Mobile environment
[16]				
[46]	Ring			
[50]		x		
[35]				Time is slotted, one event per slot
[54]	Sensors randomly scattered	x		
[13]	WSN-suitable routing			
[14]				
[24]		x		
[38]				
[18]				
[47]	Arbitrary topology			
[48]			All components are trusted	Set of authentication-encryption protocols in use
[26]				
[42]		x		
[27]				
[45]		x		
[15]				
[19]				
[32]				
[23]	Homogeneous distribution of nodes		Sink is trusted	Encrypted messages are sent periodically
[17]				
[43]				Random key distribution scheme (e.g., Gligor)
[36]			Sink is trusted	To query a sensor data: need to be registered in the sink and have a smartcard
[33]			No TTPs. Law authority has limited trust	
[37]				Key management exists
[40]				
[41]				

Table 6: Attacker-related assumptions. (∗): guessed from the text.

	Active/passive/both	Global/local	Static/moving	Insider/outsider/both	Knowledge	Behavior and capabilities	Unique/several-independent/colluding
[44]		Local	Moving				
[39]	Passive			Insider			Several
[30]							
[22]				Insider		Honest but curious	Several-colluding
[28]		Global		Outsider			
[25]	Passive	Global		Outsider			
[52]	Passive	Local	Moving	Outsider			
[29]	Passive	Global		Outsider			
[31]	Both	Global		Insider			
[21]	Passive	Semiglobal	Moving				
[34]	Passive						
[20]	Passive	Local	Moving				
[49]	Passive	Local		Insider			
[53]							
[16]	Passive	Global				Deployment and protocol-aware	Several-colluding
[46]	Passive	Global		Outsider (∗)			
[50]	Passive	Local		Outsider (∗)	Location for each ID	The same communication range as sensors	
[35]	Passive	Global		Outsider			
[54]	Passive	Local		Both		Honest but curious	Several-colluding
[13]							
[14]	Both	Multilocal	Moving	Both	Knows everything except keys and IDs	Unlimited resources (memory, processing, energy)	Several-colluding
[24]	Passive	Global		Outsider	Knows everything except keys and IDs	Unlimited resources (memory, processing, energy)	
[38]	Passive						
[18]	Passive	Global		Outsider			
[47]							
[48]	Active			Insider		Honest but curious	
[26]				Insider			Several-colluding
[42]	Both	Global				Attacker works when network is already set up	
[27]	Both			Both			
[45]							
[15]	Passive	Global		Outsider	Knows origin destination for each observed packet		Several-colluding (parallel sensor network)

Table 6: Continued.

	Active/passive/both	Global/local	Static/moving	Insider/outsider/both	Knowledge	Behavior and capabilities	Unique/several-independent/colluding
[19]	Passive	Multilocal			Sink location and crypto mechanism in use		
[32]	Active	Local		Insider		Honest but curious and dishonest	
[23]	Passive	Local	Moving	Outsider		The same communication range as sensors	
[17]	Both			Both		Honest but curious	
[43]	Passive			Both			
[36]	Active	Global		Both			
[33]	Both	Local		Both			
[37]							
[40]	Both	Global		Both			
[41]	Both	Global		Both			

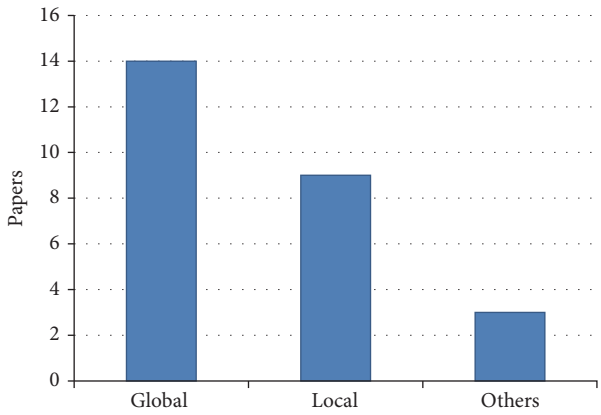

Figure 7: Attacker coverage distribution.

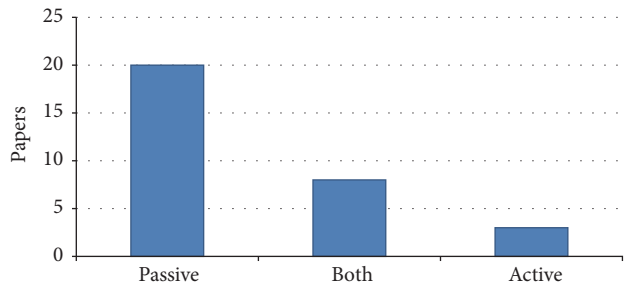

Figure 8: Attacker nature distribution.

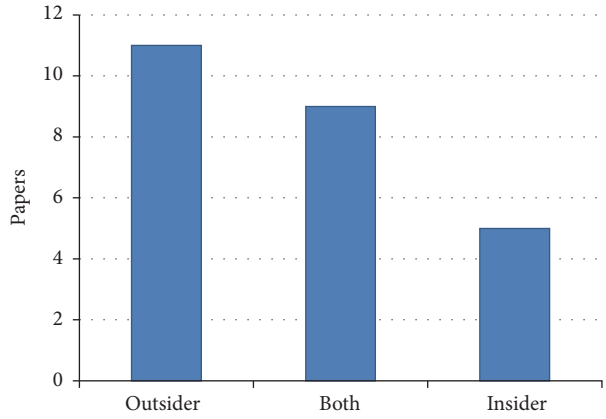

Figure 9: Attacker presence distribution.

at once. Afterwards, less papers consider that the attacker is local, meaning that the attacker only interacts with a small portion of the WSN at a time. In between global and local attackers, several settings appear. Paper [21] adopts a semiglobal attacker since authors state that a global one is not realistic. Papers [14, 19] consider a multilocal attacker, in which it may cover several network portions simultaneously.

The static/moving nature of the attacker is not relevant to global attackers, by definition. However, this is relevant to local attackers, since it makes their coverage (i.e., covered region) vary over time. In particular, [20, 23, 52] consider that attacker may be moving. Note that this is different from a multilocal attacker in that only one place may be visited at a time. Considering this aspect, the static/moving condition of the attacker should be carefully stated in papers. However, only 7 papers make this assumption explicit.

Another issue to note is how the coverage is achieved. Local attackers are sometimes assumed to have similar communication range to regular sensors (e.g., [50]). Nevertheless, in order to have global coverage, some works consider that the attacker is not a single entity but a set of colluding nodes which collectively bring this feature [15, 16]. It is noticeable that this situation cannot always be reached, since it is not always easy to manage a set of nodes within the network. Thus, this aspect should be made clear to clarify the chances for adoption for a particular use case. However, only 6 papers explicitly state it.

With respect to the attacker nature, two main classes are identified. Thus, *passive* attackers can only eavesdrop communication whereas *active* ones are able to interfere with the system itself. This distinction is made by 30 papers, which shows that the research community agrees on that this issue cannot be disregarded. Among these, passive attackers appear in most cases whereas active ones are present in the minority of them. In between, the remaining papers consider an active and passive attacker (Figure 8). Even if it could be said that active attacker capabilities already include those from the passive attacker, we have kept this distinction for the sake of clarity.

Another important dimension of the attacker is its degree of presence. In particular, *outsiders* are those attackers which perform their actions from outside the network. On the contrary, *insiders* are part of the network and may have access to other elements as any other internal member. As it happened with nature, the majority of papers qualify the attacker in this criterion (Figure 9). Among them, the majority consider outsiders whereas only a few of them adopt the insider model. The remaining papers assume that the attacker is formed by entities inside and outside the network. One important aspect is to define how many nodes are insiders. To this extent, [14] specifies that only a small portion of nodes are insiders.

The last aspect that describes an attacker is based on what it knows and which are its resources. Concerning its knowledge, [50] assumes that it knows the location for each ID. Even further, [14, 24] consider that the attacker knows everything about the system except cryptographic keys and IDs. A more relaxed version is found in [19], in which the attacker knows the sink location as well as the cryptographic system in use.

With respect to the attacker behavior, 5 papers assume an honest but curious model. This decision is tailored for internal attackers which follow the rules (e.g., the proposed mechanism) but try to guess as much information as possible. It must be noted that by definition only insider attackers may be honest but curious; outsiders cannot be honest as they are not intended to follow the proposed mechanism.

Attacker resources are also controversial. Papers [14, 24] work under the assumption that the attacker has unlimited

resources in terms of computation, battery, and storage. On the contrary, [32, 50] assume that it has the same coverage range as regular sensors.

6. Guidelines for Privacy-Related Model Definition in WSNs

Based on the observations made in the studied papers, this section focuses on proposing a set of guidelines to foster the adoption of more comprehensive and detailed models in privacy-related research works. For the sake of clarity, these suggestions are divided following the same structure as the analysis conducted in this paper. Our guidelines for privacy-related models in WSNs come in the form of a checklist for usability purposes (see Table 7).

Recalling Figure 1, the most general issues to address are goals and threats. Thus, our guidelines include two questions for each matter, aiming to spot which are the actual privacy goals, which are the data at stake, and which threats are related to data or entities.

Clarifying network and attacker assumptions involves several questions to be addressed. Thus, each of these issues are studied separately.

6.1. Network Decisions. Network-related decisions are related to the assumptions over sources, sink(s), network management, and trusted elements. For the sake of brevity, each aspect is independently covered in what follows.

Concerning sensors, most works agree on that they are resource-constrained, battery-powered devices. However, given that this technology is evolving, it is convenient to clarify the extent of these limitations. On the other hand, it is critical to define whether sensors are static, nonstatic but within a limited range, or fully mobile. This heavily impacts the suitability of approaches. Another factor to set is the distribution of nodes; if they are randomly distributed or they are arranged following some strategy.

With respect to sinks, it is commonly accepted that they are more powerful than sensors. They are sometimes qualified as unconstrained, but this category is rather unrealistic. It is advisable to determine their minimal features. Another important feature is the amount of sinks. Particularly, the less common architecture is to have several sinks. This may be an interesting research niche.

Concerning network management, the election of the topology is not straightforward. Thus, the topology at stake (e.g., ring, multiring, and tree) must be stated. On the contrary, if there is no need for a specific topology, it is convenient to clarify it. If the network has to be organized in a given way, for example, divided in clusters, it is important to determine if these clusters are statically or dynamically created. This issue has to be in consonance with the mobility of nodes and their geographical distribution.

Finally, the choice of trusted elements is a limiting factor. They set the ground base upon which the approach must be built. It is important to determine which elements belong to this condition (e.g., sensor, sink, or TTPs) and to what extent (e.g., they cannot be compromised, they cannot exfiltrate data).

6.2. Attacker-Related Decisions. Concerning the attacker-related decisions, there are two main aspects to consider: location and capabilities. Each issue is addressed below.

Related to location, the attacker placement is of utmost relevance. There are three decisions that are worth considering: its inclusion in the network, its static/nonstatic condition, and its global-local coverage. These issues differentiate against a local threat and a global one and if this condition changes over time. One related issue is to identify how the global coverage is achieved, when appropriate. If the scenario is small enough, it is reasonable to assume that it is a single entity with great coverage. However, for large-scale scenarios, it may require several-colluding nodes. Thus, stating the amount of attackers and their cooperation level is important.

With respect to the attacker capabilities, apart from the classical distinction between active and passive actions, relevant decisions must be taken regarding the attacker knowledge and behavior. Thus, it must be stated whether the attacker has some advantageous information, such as location of nodes and/or their IDs. Similarly, determining if its knowledge grows with time is important. On the other hand, the attacker behavior may follow a particular pattern, for example, honest but curious and rational/irrational. This puts a limit on the type of threats that the contribution may face.

7. Conclusion

Wireless Sensor Networks (WSNs) have received great attention in the last years. In particular, privacy preservation is of utmost importance in several application scenarios. A plethora of contributions have been produced in this regard. Although several surveys have recently focused on the internals of the proposed approaches, this paper has focused on their underlying models. Thus, the network assumptions, the considered goals, the attacker nature, and its associated threats have been analysed. For this purpose, a set of 41 papers from the last 5 years have been considered. It has been made clear that different papers take assorted decisions in these central aspects. Even worse, sometimes authors do not make explicit statements over some of these critical factors. Thus, our survey shows that many aspects remain unclear in most papers. This makes comparing approaches or even deciding whether they could be simultaneously applied impossible.

To contribute to addressing this situation, this paper has proposed a set of guidelines to build privacy-related models in WSNs. Thus, we believe that this paper will foster the adoption of more comprehensive and detailed models in future contributions from the research community.

Appendix

See Tables 1, 2, 3, 4, 5, and 6.

Table 7: Guidelines for privacy-related models in WSNs.

General issues	Goals
	Which particular aspect of privacy is at stake?
	Which kind of data are privacy-sensitive?
	Threats
	Which are the data privacy threats (if any)?
	Which are the entity privacy threats (if any)?
Network decisions	Sensor
	How limited their resources are?
	May they move? If so, are there any boundaries?
	Are they placed following any strategy or randomly scattered?
	Sink
	How many of them are there?
	If they are several, do they cooperate?
	How powerful is it?
	Network
	Is any topology assumed (e.g., ring, tree) or it may work for any topology?
	Is the network organized in some way (e.g., cluster, areas)?
	If so, is this organization permanent?
	Trusted elements
	Are sensors trusted? If so, to what extent?
	Are sinks trusted? If so, to what extent?
	Are communications trusted? Which ones (e.g., sensor-sensor, sensor-sink, and sensor-user)? To what extent?
	Are there Trusted Third Parties? If so, what are they trusted for?
Attacker-related decisions	Coverage
	Where is it placed? Is it internal, external, or both?
	Does it have global view? If so, how?
	Does it move over time?
	Nature
	Is it active, passive, or both?
	Presence
	If it involves internal nodes, is there any upper/lower limit?
	Knowledge
	Which information does it know? Does this information change over time?
	Behavior and resources
	Does it have any attack pattern? Is it honest?
	Does it attack for a given benefit to a particular subset of nodes?
	If it involves several entities, do they cooperate? To what extent?

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the MINECO Grant TIN2013-46469-R (Security and Privacy in the Internet of You (SPINY)) and the CAM Grant S2013/ICE-3095 (Cybersecurity, Data, and Risks (CIBERDINE)), which is cofunded by European Funds (FEDER). Furthermore, J. M. de Fuentes and L. González-Manzano were also partially supported by the Programa de Ayudas a la Movilidad of Carlos III University of Madrid.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[3] C. Y. Chow, W. Xu, and T. He, "Privacy enhancing technologies for wireless sensor networks," in *The Art of Wireless Sensor Networks*, pp. 609–641, Springer, 2014.

[4] A. Tayebi, S. Berber, and A. Swain, "Wireless sensor network attacks: an overview and critical analysis," in *Proceedings of the 7th International Conference on Sensing Technology (ICST '13)*, pp. 97–102, Wellington, New Zealand, December 2013.

[5] R. Rios, J. Lopez, and J. Cuellar, "Location privacy in WSNs: solutions, challenges, and future trends," in *Foundations of Security Analysis and Design VII*, vol. 8604 of *Lecture Notes in Computer Science*, pp. 244–282, Springer, 2014.

[6] P. Gupta and M. Chawla, "Privacy preservation for WSN: a survey," *International Journal of Computer Applications*, vol. 48, no. 3, pp. 11–16, 2012.

[7] N. Oualha and A. Olivereau, "Sensor and data privacy in industrial wireless sensor networks," in *Proceedings of the Conference on Network and Information Systems Security*, pp. 1–8, 2011.

[8] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1238–1280, 2013.

[9] R. Bista and J.-W. Chang, "Privacy-preserving data aggregation protocols for wireless sensor networks: a survey," *Sensors*, vol. 10, no. 5, pp. 4577–4601, 2010.

[10] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.

[11] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.

[12] K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: a survey," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 42, no. 6, pp. 1243–1256, 2012.

[13] D. Christin, A. Reinhardt, SS. Kanhere, and M. Hollick, "Fine-grained access control enabling privacy support in wireless sensor networks," in *Proceedings of the 9th KuVS Fachgespräch Drahtlose Sensornetze*, vol. 1, pp. 29–32, Würzburg, Germany, September 2010.

[14] A.-S. Abuzneid, T. Sobh, M. Faezipour, A. Mahmood, and J. James, "Fortified anonymous communication protocol for location privacy in WSN: a modular approach," *Sensors*, vol. 15, no. 3, pp. 5820–5864, 2015.

[15] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2012.

[16] A. Debnath, P. Singaravelu, and S. Verma, "Efficient spatial privacy preserving scheme for sensor network," *Central European Journal of Engineering*, vol. 3, no. 1, pp. 1–10, 2013.

[17] C. Ma, K. Xue, and P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks," *Security and Communication Networks*, vol. 7, no. 4, pp. 759–773, 2014.

[18] B. Di Ying, D. Makrakis, and H. T. Mouftah, "Anti-traffic analysis attack for location privacy in WSNs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, article 131, 2014.

[19] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.

[20] J. Long, M. Dong, K. Ota, and A. Liu, "Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks," *IEEE Access*, vol. 2, pp. 633–651, 2014.

[21] M. Raj, N. Li, D. Liu, M. Wright, and S. K. Das, "Using data mules to preserve source location privacy in Wireless Sensor Networks," *Pervasive and Mobile Computing*, vol. 11, no. 1, pp. 244–260, 2014.

[22] M. M. Groat, W. Hey, and S. Forrest, "KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks," in *Proceedings of the IEEE INFOCOM*, pp. 2024–2032, IEEE, Shanghai, China, April 2011.

[23] W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in WSNs based on path extension," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 461–471, 2014.

[24] Y. Yang, M. Shao, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor Networks," *ACM Transactions on Sensor Networks*, vol. 9, no. 3, article 34, Article ID 2480737, 2013.

[25] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Toward a statistical framework for source anonymity in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 248–260, 2013.

[26] J. Wu and F. Zhang, "Privacy-preserving regression modeling and attack analysis in sensor network," in *Cloud Computing and Big Data*, W. Qiang, X. Zheng, and C.-H. Hsu, Eds., vol. 9106 of *Lecture Notes in Computer Science*, pp. 354–366, Springer, New York, NY, USA, 2015.

[27] E. C.-H. Ngai and I. Rodhe, "On providing location privacy for mobile sinks in wireless sensor networks," *Wireless Networks*, vol. 19, no. 1, pp. 115–130, 2013.

[28] C.-Y. Chow, M. F. Mokbel, and T. He, "A privacy-preserving location monitoring system for wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 94–107, 2011.

[29] S. Ortolani, M. Conti, B. Crispo, and R. Di Pietro, "Events privacy in WSNs: a new model and its application," in *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '11)*, pp. 1–9, IEEE, Lucca, Italy, June 2011.

[30] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 2, article 14, pp. 1–12, 2010.

[31] L. Buttyán and T. Holczer, "Perfectly anonymous data aggregation in wireless sensor networks," in *Proceedings of the IEEE 7th International Conference on Mobile Ad hoc and Sensor Systems (MASS '10)*, pp. 513–518, November 2010.

[32] X. Liao and J. Li, "Privacy-preserving and secure top-k query in two-tier wireless sensor network," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 335–341, IEEE, Anaheim, Calif, USA, December 2012.

[33] D. He, S. Chan, and M. Guizani, "Accountable and privacy-enhanced access control in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 389–398, 2015.

[34] J.-H. Park, Y.-H. Jung, H. Ko, J.-J. Kim, and M.-S. Jun, "A privacy technique for providing anonymity to sensor nodes in a sensor network," *Communications in Computer and Information Science*, vol. 150, no. 1, pp. 327–335, 2011.

[35] Y. Zhang, M. Price, L. Opyrchal, and K. Frikken, "All Proxy Scheme for event source anonymity in wireless sensor networks," in *Proceedings of the 6th International Conference on*

Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '10), pp. 263–268, IEEE, Brisbane, Australia, December 2010.

[36] P. Kumar, A. Gurtov, M. Ylianttila, S.-G. Lee, and H. J. Lee, "A strong authentication scheme with user privacy for wireless sensor networks," *ETRI Journal*, vol. 35, no. 5, pp. 889–899, 2013.

[37] N. Bruce, Y. S. Lee, S. G. Lee, and H. J. Lee, "A privacy preserving security protocol-based application for wireless communication system," in *Proceedings of the IEEE 17th International Conference on High Performance Computing and Communications (HPCC '15), the IEEE 7th International Symposium on Cyberspace Safety and Security (CSS '15) and the IEEE 12th International Conference on Embedded Software and Systems (ICESS '15)*, pp. 1651–1656, New York, NY, USA, August 2015.

[38] L. Zhou, Q. Wen, and H. Zhang, "Protecting sensor location privacy against adversaries in wireless sensor networks," in *Proceedings of the 5th International Conference on Computational and Information Sciences (ICCIS '13)*, pp. 1384–1387, Shiyang, China, June 2013.

[39] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *Proceedings of the IEEE INFOCOM*, pp. 1–9, March 2010.

[40] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and integrity for data aggregation in WSN using homomorphic encryption," *Wireless Personal Communications*, vol. 80, no. 2, pp. 867–889, 2014.

[41] K. Xie, X. Ning, X. Wang et al., "An efficient privacy-preserving compressive data gathering scheme in WSNs," in *Algorithms and Architectures for Parallel Processing*, G. Wang, A. Zomaya, G. M. Perez, and K. Li, Eds., vol. 9528 of *Lecture Notes in Computer Science*, pp. 702–715, Springer, New York, NY, USA, 2015.

[42] R.-H. Hu, X.-M. Dong, and D.-L. Wang, "Protecting data source location privacy in wireless sensor networks against a global eavesdropper," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 492802, 17 pages, 2014.

[43] G. Yang, S. Li, X. Xu, H. Dai, and Z. Yang, "Precision-enhanced and encryption-mixed privacy-preserving data aggregation in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, Article ID 427275, pp. 1–12, 2013.

[44] X. Luo, X. Ji, and M.-S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *Proceedings of the International Conference in Information Science and Applications (ICISA '10)*, pp. 1–6, Seoul, South Korea, April 2010.

[45] B. Ntirenganya, Z. Zhang, L. Zhu, Y.-A. Tan, Z. Yang, and C. Guo, "Enhanced privacy preserving pattern-code based data aggregation in wireless sensor networks," in *Proceedings of the 9th IEEE International Conference on Mobile Ad-Hoc and Sensor Networks (MSN '13)*, pp. 336–341, December 2013.

[46] L. Yao, L. Kang, F. Deng, J. Deng, and G. Wu, "Protecting source-location privacy based on multirings in wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 15, pp. 3863–3876, 2015.

[47] J. E. Tapiador, M. Srivatsa, J. A. Clark, and J. A. McDermid, "Decorrelating WSN traffic patterns with maximally uninformative constrained routing," in *NETWORKING 2011 Workshops*, vol. 6827 of *Lecture Notes in Computer Science*, pp. 207–218, Springer, Berlin, Germany, 2011.

[48] X. Yang, X. Ren, S. Yang, and J. McCann, "A novel temporal perturbation based privacy-preserving scheme for real-time monitoring systems," *Computer Networks*, vol. 88, pp. 72–88, 2015.

[49] C. Li and Y. Liu, "ESMART: energy-efficient slice-mix-aggregate for wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 134509, 9 pages, 2013.

[50] A. Gurjar and A. R. B. Patil, "Cluster based anonymization for source location privacy in wireless sensor network," in *Proceedings of the 3rd International Conference on Communication Systems and Network Technologies (CSNT '13)*, pp. 248–251, IEEE, Gwalior, India, April 2013.

[51] A. Back, U. Möller, and A. Stiglic, "Traffic analysis attacks and trade-offs in anonymity providing systems," in *Information Hiding*, I. S. Moskowitz, Ed., vol. 2137 of *Lecture Notes in Computer Science*, pp. 245–257, Springer, London, UK, 2001.

[52] L. Yao, L. Kang, P. Shang, and G. Wu, "Protecting the sink location privacy in wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 883–893, 2013.

[53] K.-J. Kim and S.-P. Hong, "Privacy care architecture in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, Article ID 369502, 2013.

[54] X. Zhang, H. Chen, K. Wang, H. Peng, Y. Fan, and D. Li, "Rotation-based privacy-preserving data aggregation in wireless sensor networks," in *Proceedings of the 1st IEEE International Conference on Communications (ICC '14)*, pp. 4184–4189, IEEE, Sydney, Australia, June 2014.